

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

(1) Residence located at 1839 18th Avenue, Kenosha, WI 53140-1644, including any detached or outbuildings. (2) 2013 Gray Ford F-150, with WI license plate TY9002. (3) the person of Charles Diel, DOB 04/21/1968. Further description can be found in Attachment A.

Case No.23-943M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (*identify the person or describe the property to be seized*):

Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 7/20/2023 *(not to exceed 14 days)*

xx ☐ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*)

☐ for _____ days (*not to exceed 30*) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 7/6/2023 @ 8:54 a.m.

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

Attachment A

Description of Subject Premises, Subject Vehicle, and Subject Person

1. 1839 18th Ave, Kenosha, WI 53140, the SUBJECT PREMISES, is described as a single-family ranch style home. The residence has blue siding with a half gray brick veneer on the front. There are three windows and a door on the front of the house and a driveway leading to a detached garage in the back. The detached garage has matching siding with the house and a white garage door. The backyard has a chain link fence. The front door has the house number "1839" visible on a sign. (below picture from Google)



2. 2013 Gray Ford F-150 with Wisconsin license plate TY9002
3. Person of Charles Diel, date of birth April 21, 1968

Attachment B

Items To Be Seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252(a)(2) and (a)(4):

1. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of any electronic messaging application;

e. Records and information related to any money transfer or other payment systems; and

f. Records and information showing access to and/or use of any electronic messaging application.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the SUBJECT PREMISES, and vehicles associated with the SUBJECT PREMISES, described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the SUBJECT PREMISES or Subject Vehicle to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad or fingerprint scanner or reader of other devices found at the SUBJECT PREMISES or Subject Vehicle for the purpose of attempting to unlock the device via Touch ID/fingerprint scanner or reader in order to search the contents as authorized by this warrant.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Case No.23-943M(NJ)

(1) Residence located at 1839 18th Avenue, Kenosha, WI 53140-1644,
including any detached or outbuildings. (2) 2013 Gray Ford F-150, with WI
license plate TY9002. (3) the person of Charles Diel, DOB 04/21/1968.
Further description can be found in Attachment A.

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Please see Attachment A.

located in the _____ Eastern _____ District of _____ Wisconsin _____, there is now concealed (identify the person or describe the property to be seized):

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

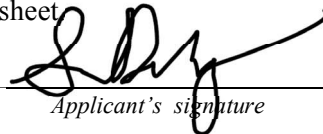
Code Section	Offense Description
18 U.S.C. 2251(a)	Attempted Production of Child Pornography
18 U.S.C. 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

Please see attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Sarah Dettmering, Special Agent, FBI

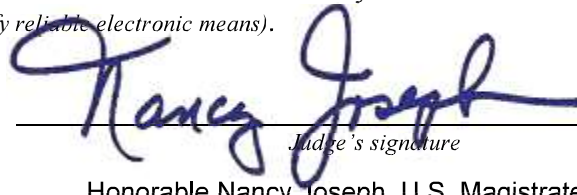
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

TELEPHONE

(specify reliable electronic means).

Date: 7/6/2023



Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Sarah Dettmering, being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since January 2018 and am currently assigned to the Milwaukee Division as a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. My duties include investigating criminal violations relating to child sexual exploitation and child pornography. While employed by the FBI, I have investigated federal criminal violations related to child exploitation and child pornography. I have received training from the FBI specific to investigating child pornography and child exploitation crimes and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media. As a result of my training, experience, and discussions with other law enforcement officers assigned to investigate child pornography and child exploitation, I am familiar with methods by which electronic devices are used as the means for receiving, transmitting, possessing, and distributing images and videos depicting minors engaged in sexually explicit conduct. I have also received training and gained experience in interview and interrogation techniques with enhanced training specific to cybercrimes, social media search warrants, residential search warrants, interviews and interrogations of subjects of criminal investigations, electronic device identification and forensic review.

2. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other law

enforcement officers, who have provided information to me during the course of their official duties and whom I consider truthful and reliable.

3. Based upon the information described below, I submit that probable cause exists to believe that Charles Diel was the user of the Snapchat account in the name of “daddy531968” (SUBJECT ACCOUNT 1) and the Kik account in the name of “daddcumplay_245” (SUBJECT ACCOUNT 2), collectively “SUBJECT ACCOUNTS” and has committed the crimes of attempted production of child pornography, in violation of Title 18, United States Code, Section 2251(a)(2) and possession of child pornography in violation of Title 18, United States Code, Section 2252(a)(4)(B). I further submit that evidence relating to this crime, more particularly described in Attachment B, can be found at Diel’s residence 1839 18th Ave, Kenosha, WI 53140-1644 including any detached or outbuildings (SUBJECT PREMISES), in Diel’s vehicle, a 2013 Gray Ford F-150 with Wisconsin license plate TY9002, and on Diel’s person, more particularly described in Attachment A. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

DEFINITIONS

4. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

a. “Child Pornography” is defined in 18 U.S.C. § 2256 as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to

appear that an identifiable minor is engaged in sexually explicit conduct. Child pornography is also commonly referred to as Child Sexual Abuse Material, or “CSAM.”

b. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. “An Internet Protocol address” (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static that is, long-term IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

e. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

f. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

g. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

h. “Visual depictions” include undeveloped film and videotape, and data stored on a computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

i. “Website” consists of text pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol.

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

5. I am aware through training, experience, and consulting with other law enforcement agents/analysts with specialized knowledge and training in computers, networks, and Internet communications that to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the electronic storage devices. To ensure such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, within a hand-held electronic device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of this electronic information, as explained below, might take a form that becomes meaningful only upon forensic analysis.

6. Based on my knowledge, training, and experience, I know that computer and other electronic device hardware, peripheral devices, software, documentation, and passwords may be important to a criminal investigation in three distinct and important respects:

- a. The objects themselves may be instrumentalities used to commit the crime.
- b. The objects may have been used to collect and store information about crimes (in the form of electronic data).

c. The objects may be contraband or fruits of the crime.

7. I submit that if a computer or other electronic storage device is found on the premises, there is probable cause to believe those records will be stored in that electronic storage device, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person deletes a file on an electronic storage device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. It follows that deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone, or tablet device) the device may also contain a record of deleted data in a swap or recovery file.

b. Wholly apart from user-generated files, electronic storage device storage media in particular, computers' internal hard drives, contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users typically do not erase or delete this evidence

because special software is typically required for that task. However, it is technically possible to delete this information.

c. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

8. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how electronic storage devices were used, the purpose of their use, who used them, and when.

9. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device was remotely accessed, thus inculcating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, as described herein, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also

contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic and timeline information described herein may either inculcate or exculpate the electronic storage device user. Last, information stored within an electronic storage device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer

user's knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

10. Based upon my knowledge, training and experience, and after having consulted with FBI computer forensic personnel, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some electronic storage device equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

11. In light of these concerns, I hereby request the Court's permission to seize the electronic storage devices, associated storage media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

12. I know that when an individual uses a computer to commit crimes involving child pornography, the individuals' computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage device is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe that an electronic storage device used to commit a crime of this type may contain data that is evidence of how the electronic storage

device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

BIOMETRIC ACCESS TO DEVICES

13. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

14. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

15. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes

and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

16. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

17. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

18. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices,

making the use of biometric features necessary to the execution of the search authorized by this warrant.

19. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

20. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, I request authority for law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of DIEL, to the fingerprint scanner of the devices found on DIEL or at the SUBJECT PREMISES or in the SUBJECT VEHICLE; (2) hold the devices found on DIEL, in the SUBJECT VEHICLE or at the SUBJECT PREMISES in front of DIEL's face to activate the facial recognition feature; and/or (3) hold the devices found on DIEL, in the SUBJECT VEHICLE or at the SUBJECT PREMISES in front of DIEL's face and activate the iris recognition

feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

BACKGROUND ON KIK

21. Kik is a free instant-messaging application for mobile devices. Kik uses a mobile device's data plan or Wi-Fi to transmit and receive messages. Kik allows users to share photographs, sketches, mobile webpages, linked internet files, and other content. To use this application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded and installed, the user is prompted to create an account and username. The user also has a display name, which is what other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature and the two parties can then send each other messages, images, and videos.

22. During the registration process, Kik registers date, time, internet protocol (IP) address, and device related information. The username is the only unique identifier used by Kik. According to the Kik Law Enforcement Guide, a Kik username is unique and can never be replicated or changed. Kik users are also able to create chat groups of up to 50 people to communicate in a group setting and exchange images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the group. Once the group is created, Kik users can share a link to the group with any other Kik user.

BACKGROUND ON SNAPCHAT

23. Snapchat is a mobile application made by Snap Inc. and available through the iPhone App Store and Google Play Store. The Snapchat app provides users a way to share moments with photos, videos, and chats.

24. Snaps are photos or videos taken using the Snapchat app's camera on an individual's mobile device, and may be shared directly with the user's friends, or in a Story (explained below) or Chat. Snap Inc.'s servers are designed to automatically delete a Snap after it has been opened by all intended recipients. Snap's servers are designed to automatically delete an unopened Snap sent directly to a recipient after 30 days and an unopened Snap in Group Chat after 24 hours.

25. A user can add Snaps to their "Story". A Story is a collection of Snaps displayed in chronological order. Users can manage their privacy settings so that their Story can be viewed by all Snapchatters, their friends, or a custom audience. A user can also submit their Snaps to our crowd-sourced service "Our Story", which enables their Snaps to be viewed by all Snapchatters in Search and Snap Map. Snap Inc.'s servers are designed to automatically delete a Snap in a user's Story 24 hours after the user posts the Snap, but the user may delete part or all of the Story earlier. Submissions to Our Story may be saved for longer periods of time.

26. Memories is Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. Content saved in Memories is backed up by Snap Inc. and may remain in Memories until deleted by the user. Users may encrypt their content in Memories (called "My Eyes Only"), in which case the content is not accessible to Snap Inc and cannot be decrypted by Snap Inc.

27. A user can type messages, send Snaps, audio notes, and video notes to friends within the Snapchat app using the Chat feature. Our servers are designed to automatically delete one-to-one chats once the recipient has opened the message and both the sender and recipient have left the chat screen, depending on the user's chat settings. Snap Inc.'s servers are designed to automatically delete unopened one-to-one chats in 30 days. Users can also chat in groups. Chats sent in groups are deleted after 24 hours whether they are opened or not. A user can save a message in Chat by pressing and holding the message. The user can un-save the message by pressing and holding it again. This will delete it from Snap Inc.'s servers. Users can also delete chats that they have sent to a recipient before the recipient has opened the chat or after the recipient has saved the chat.

28. If a user has device-level location services turned on and has opted into location services on Snapchat, Snap Inc. will collect location data at various points during the user's use of Snapchat, and retention periods for location data vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the app settings.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

29. On or about March 21, 2023, an FBI Online Covert Employee (FBI-OCE) obtained consent to assume the online identity of a minor female ("MF"), date of birth June 2007, using the girl's Snapchat account ("VICTIM ACCOUNT").

30. FBI-OCE reviewed the contents of the VICTIM ACCOUNT which showed that MF communicated with SUBJECT ACCOUNT 1, with the earliest visible message on February 3, 2023. SUBJECT ACCOUNT 1's display name on Snapchat was "Cumplay[devil emoji][devil emoji][fire emoji][fire emoji]."

31. Further review of the VICTIM ACCOUNT showed that MF sent multiple images and videos to the SUBJECT ACCOUNT 1 which are consistent with the definition of Child Sexual Abuse Material (CSAM). These images had been saved in the chat. The user of SUBJECT ACCOUNT 1 sent multiple images of an adult male's penis and videos of an adult male masturbating. These images were also saved in the chat.

32. FBI-OCE provided a screen-recording of the Snapchat chats between the VICTIM ACCOUNT and SUBJECT ACCOUNT 1 to FBI Milwaukee, and I subsequently reviewed them. The dates and times indicated in the following paragraphs are what was shown in the screen-recording of the VICTIM ACCOUNT, it is likely these times are not in Central Standard Time.

33. The first saved image in the chats between the VICTIM ACCOUNT and SUBJECT ACCOUNT 1 was dated February 3, 2023, and the time stamp showed 10:39 PM. This image showed a minor female, approximately fourteen (14) to sixteen (16) years old, taking a picture of herself in a mirror with her shirt pulled up to expose her chest. The girl was wearing a bra. Shortly after, a further eight (8) sexually explicit images were sent by the VICTIM ACCOUNT. At approximately 10:51 PM the SUBJECT ACCOUNT 1 sent an image of an adult male's penis.

34. On or about February 4, 2023, at approximately 8:24 AM SUBJECT ACCOUNT 1 sent the VICTIM ACCOUNT a video of an adult male masturbating.

35. The SUBJECT ACCOUNT 1 and the VICTIM ACCOUNT continued to share explicit images and videos with each other. On or about February 9, 2023, at approximately 7:44 PM the VICTIM ACCOUNT sent SUBJECT ACCOUNT 1 a video of a minor female, approximately fourteen (14) to sixteen (16) years old, completely nude. The girl rubbed her exposed breasts, then spreads her legs and rubbed her nude vagina.

36. On or about March 2, 2023 (the time stamp was not visible on this video) the VICTIM ACCOUNT sent a video to the SUBJECT ACCOUNT 1 of a minor female, approximately fourteen (14) to sixteen (16) years old, sitting with her legs spread, and her underwear pulled to the side to expose her nude vagina to the camera. The girl was inserting what appeared to be a black comb into her vagina.

37. On or about April 3, 2023, through approximately April 4, 2023, after FBI-OCE had assumed operation of the VICTIM ACCOUNT, the VICTIM ACCOUNT (VA) re-engaged with SUBJECT ACCOUNT 1 (SA1) and the following chat exchange took place:

VA: Hey

SA1: Hi baby girl how r u

SA1: R u going to say hi lol

VA: Hi. Was grounded. Hate being 16

VA: I hate my parents and sick of fucking school

SA1: I'm sorry r u still grounded

VA: Not really

SA1: Oh nice what u up to

VA: No much but my parents r all over my ass

VA: Do u have Kik?

VA: I rather chat on that

SA1: Aww I'm sorry. Yess I do may I ask y lol.

SA1: daddcumplay is mine

VA: I'll txt on that in a bit and explain

SA1: No worries sweetie

SA1: Ok

38. FBI-OCE subsequently began to communicate with SUBJECT ACCOUNT 2 via Kik. FBI-OCE provided FBI Milwaukee with the Kik chats between FBI-OCE and SUBJECT ACCOUNT 2, which I then reviewed. These chats do not have date and time stamps on them.

39. During the Kik chat between FBI-OCE (FO) and SUBJECT ACCOUNT 2 (SA2) the following exchange took place, where FBI-OCE reiterated that FBI-OCE was sixteen (16) years old:

FO: I hate being 16
SA2: Do u think they saw anything
SA2: I know lol
FO: No I don't
SA2: That's good
FO: Literally 16 sucks
SA2: I know I've been there A long time ago though lol
FO: R u talking about the vids we sent each other
SA2: Yess
FO: I hope they didn't
SA2: Me too lol
SA2: U r daddy's good girl

40. After these messages, where FBI-OCE stated multiple times that FBI-OCE was sixteen (16) years old, SUBJECT ACCOUNT 2 sent FBI-OCE multiple requests for images/videos which would be consistent with the definition of CSAM. Examples of these chat exchanges are described below:

SA2: Welcome. What u wearing this evening sweetie lol
FO: Just a tshirt
SA2: Really no panties lol
FO: Haha no
SA2: Mmm yess can daddy see lol
FO: See what daddy
SA2: U in your shirt with no panties lol

...

SA2: Daddy getting hard damn I've missed u baby girl
FO: Haha how hard
SA2: Show me your tits I'll show u
FO: Doing a vid
SA2: Maybe lol. If u play with nipples
FO: I will

SA2: Mmm. Good girl

...

SA2: Play with your nipples make daddy cum

SA2: [SA2 sent a sexually explicit image of an adult male]

SA2: Precum just for u baby girl

FO: Yum

SA2: Wish u were here to lick it off

...

FO: Where u live again

SA2: Wisconsin

FO: Oh lol I thought it was Ohio for some reason

SA2: Can daddy see your tits baby girl. Lol close

...

SA2: What u wearing today baby girl

FO: Nothing still in bed

SA2: Mmm nice lol daddy see

FO: Like what u want to see lol

FO: Pic or vid

SA2: you laying in bed naked or video would be hot

FO: What does daddy wanna c in the vid

SA2: Daddy love to see you play with your nipples

FO: What else

SA2: Then lick your fingers and play with your nipples for daddy you know what no play with you pussy for daddy get your fingers, good and wet and then play with your nipples with your wet fingers

FO: Anything else

SA2: Maybe then grab your hairbrush and fuck your sweet young wet pussy with your airbrush like daddy would with my hard cock

FO: Ok I'll do it daddy

SA2: Mmm yess that's daddy's good girl. Damn wish I was there to watch live

FO: K I make it

SA2: Yess please make it for daddy

FO: It's done

SA2: Mmmmm yess good girl.

FO: I even moaned daddy

SA2: Omfg yess luv to see

41. On or about April 5, 2023, the minor female victim (MF) participated in a Child and Adolescent Forensic Interview (CAFI). FBI-OCE provided the following information pertaining to the CAFI to FBI Milwaukee:

- a. During the CAFI the MF was shown a selfie image that was sent by SUBJECT ACCOUNT 1 which showed an adult male.
- b. MF recognized the image as a man that MF chatted with on Snapchat.
- c. MF told the male that MF was sixteen (16) years old.
- d. MF discussed going on a school field trip during the chats.
- e. MF sent nude photographs of MF's genitals to the male and the male sent nude photographs of his genitals to MF.

42. The above-described communications between the VICTIM ACCOUNT and the SUBJECT ACCOUNTS show that the user of the SUBJECT ACCOUNTS possessed CSAM and also requested an individual who the user believed to be under the age of 18 to produce CSAM.

IDENTIFICATION OF THE SUBJECT

43. The male operating the SUBJECT ACCOUNTS was identified as Charles Diel, date of birth April 21, 1968.

44. While operating SUBJECT ACCOUNT 1 Diel sent multiple selfie style images which showed his face. These images bore a strong resemblance to Diel's driver's license image and I believe they are the same person.

45. Per the results of an administrative subpoena served on Kik for information associated with SUBJECT ACCOUNT 2, the email address associated with SUBJECT ACCOUNT 2 was cddiel@wi.rr.com and multiple login IP addresses were 74.135.253.112.

46. This email address, cddiel@wi.rr.com, was also associated with a publicly visible Facebook page for a business called “Woodchuck’s Woodshed” which in the “Bio” section stated “Custom woodworking projects. See something you like let’s us know how we can customize it to fit y.” During the Snapchat conversation between SUBJECT ACCOUNT 1 and MF, the SUBJECT ACCOUNT 1 sent MF multiple images of woodworking projects. The publicly visible Facebook account in the name of “Chuck Diel” showed images of an adult male who bore a strong resemblance to the male in the selfies shared by SUBJECT ACCOUNT 1 and Diel’s driver’s license images and I believe them to be the same person. “Chuck Diel’s” Facebook page showed that he was the Owner and CEO of Woodchuck’s Woodshed and lived in Kenosha Wisconsin.

47. The IP address associated with multiple Kik logins, 74.135.253.112, was registered to Charter Communications Inc (Charter). An administrative subpoena was served on Charter and on or about April 17, 2023 Charter provided the following information in the response:

- a. Subscriber Name: Charles Diel
- b. Service Address: 1839 18th Ave, Kenosha, WI 53140-1644 [SUBJECT PREMISES]
- c. User Name or Features: cddiel@wi.rr.com, cdiel@wi.rr.com, Kathy.diel@wi.rr.com, kcdiel@wi.rr.com
- d. Phone Number: 262-914-1968
- e. Lease Log: Start Date 05/24/2022 10:24 PM End Date 04/12/2023 07:52 PM

48. FBI Special Agents conducted surveillance on multiple occasions at the SUBJECT PREMISES and observed Diel at the residence. The following observations were made on the dates listed:

a. On or about June 1, 2023, Diel was observed driving the SUBJECT VEHICLE, which was registered to Diel with the registration address listed as the SUBJECT PREMISES. The SUBJECT VEHICLE was observed at an auto parts business. At approximately 12:46 PM Diel was observed entering the SUBJECT VEHICLE as the driver. At approximately 1:00 PM the SUBJECT VEHICLE was observed at the SUBJECT PREMISES.

b. On or about June 6, 2023, at approximately 6:10 AM the SUBJECT VEHICLE was observed driving away from the TARGET RESIDENCE, at approximately 6:21 AM the SUBJECT VEHICLE arrived at an auto parts business and Diel was observed exiting the SUBJECT VEHICLE.

49. Based upon the above provided information, including the matching images of the operator of the SUBJECT ACCOUNT 1 and known images of Diel, as well as the IP addresses used for the SUBJECT ACCOUNT 2 being registered to the home address of Diel, there is probable cause to believe that Diel was the user of the SUBJECT ACCOUNTS and evidence of violations of federal law can be found at the SUBJECT PREMISES, on Diel's person and in the SUBJECT VEHICLE.

**BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE
INTERNET**

50. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers, cellular telephones, and other electronic storage devices (collectively electronic storage devices) have dramatically changed the way in which individuals interested in child pornography interact with each other. Electronic storage devices basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a device by simply connecting the camera to the electronic storage device. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store terabytes of data, which provides enough space to store thousands of high-resolution photographs. Video recorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the video recorder to a computer. Many electronic storage devices (e.g., computers, cellular telephones, and tablets), have cameras built into the device which allows users to create and store still and video images on the device. Moreover, if the device has internet connectivity, users can distribute still and video images from the device.

c. Internet-enabled electronic storage devices can connect to other internet-enabled devices the world over. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically

changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to an internet-enabled electronic storage device. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), and easy access to the Internet, electronic storage devices are the preferred method of distribution and receipt of child pornographic materials.

d. Electronic storage devices are the ideal repository for child pornography. The amount of information that an electronic storage device can hold has grown exponentially over the last decade. Electronic storage devices can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on a computer or other electronic storage device. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Many electronic storage devices can easily be concealed and carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Google, among

others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any internet-enabled electronic storage device. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's electronic storage device in most cases.

g. As is the case with most digital technology, communications by way of electronic storage device can be saved or stored on the device. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, an electronic storage device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

h. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

51. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage.

52. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

53. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who transport, distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

d. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

e. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Such individuals prefer not to be without their child pornography for any prolonged period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if an individual uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in the SUBJECT PREMISES, SUBJECT VEHICLE or a device located on Diel, as set forth in Attachment A.

CONCLUSION

54. I respectfully request that this Court issue a search warrant for the location, vehicle and search of person described in Attachment A authorizing the seizure and search of the items described in Attachment B.

Attachment A

Description of Subject Premises, Subject Vehicle, and Subject Person

1. 1839 18th Ave, Kenosha, WI 53140, the SUBJECT PREMISES, is described as a single-family ranch style home. The residence has blue siding with a half gray brick veneer on the front. There are three windows and a door on the front of the house and a driveway leading to a detached garage in the back. The detached garage has matching siding with the house and a white garage door. The backyard has a chain link fence. The front door has the house number "1839" visible on a sign. (below picture from Google)



2. 2013 Gray Ford F-150 with Wisconsin license plate TY9002
3. Person of Charles Diel, date of birth April 21, 1968

Attachment B

Items To Be Seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252(a)(2) and (a)(4):

1. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of any electronic messaging application;

e. Records and information related to any money transfer or other payment systems; and

f. Records and information showing access to and/or use of any electronic messaging application.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the SUBJECT PREMISES, and vehicles associated with the SUBJECT PREMISES, described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the SUBJECT PREMISES or Subject Vehicle to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad or fingerprint scanner or reader of other devices found at the SUBJECT PREMISES or Subject Vehicle for the purpose of attempting to unlock the device via Touch ID/fingerprint scanner or reader in order to search the contents as authorized by this warrant.